



# Department of Homeland Security Daily Open Source Infrastructure Report for 19 July 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- Reuters reports the Midwest Independent Transmission System Operator on Monday, July 17, called an emergency alert for conservation in its western region, in response to extreme heat causing record power demand. (See item [3](#))
- The Associated Press reports the Department of Homeland Security is requesting specific lists of Louisiana's shelters, immobile hospital patients, and transportation pickup points before it can promise reliable evacuation help during a major hurricane. (See item [20](#))

### DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 18, Washington Times* — **Utilities confident they can handle heat.** Electricity demand in the mid-Atlantic region Monday, July 17, broke the peak usage record set last summer, but area utility companies said they are equipped to handle this week's heat wave. "We have already exceeded the peak record that we set last summer and usage continues to climb," said Ray Dotter, spokesperson for PJM, which operates the power grid on behalf of electric companies in the District and parts of 13 states, including Maryland and Virginia. Dotter said he did not think area residents will have to cope with any brownouts — or voltage reductions — this week. The Washington area's three electric companies said they will be able to meet this

week's high demand but called for customers to conserve energy. Pepco's two reserve power plants were operating Monday. The plants operate fewer than 20 days a year and kick in during periods of extreme heat or cold to meet spikes in demand. Dominion had most of its 27 reserve plants operating Monday, said Dan Genest, a spokesperson for the Richmond utility company. He did not think a voltage reduction would be necessary this week.

Source: <http://www.washtimes.com/functions/print.php?StoryID=20060717-100059-5594r>

2. *July 17, Bloomberg* — **Australia may become energy supply superpower, prime minister says.** Australia has the potential to become an energy "superpower," with an increased share of global coal, natural gas, and uranium trade, said Prime Minister John Howard. Australia is the world's largest coal exporter and may become the second-largest liquefied natural gas exporter by 2015, Howard said Monday, July 17, in a speech to the Committee for Economic Development of Australia in Sydney. The country also holds about 40 percent of the world's known low-cost uranium reserves amid increasing demand for the nuclear fuel, he said. Australia's energy exports are forecast to increase to about \$34 billion in the year ending June 30. Global energy demand may jump by more than 50 percent by 2030 from 2003, with most demand growth coming from faster growing developing countries such as China and India, the International Energy Agency estimates.

Source: [http://www.bloomberg.com/apps/news?pid=20601081&sid=a5qxXvmV\\_fIBQ](http://www.bloomberg.com/apps/news?pid=20601081&sid=a5qxXvmV_fIBQ)

3. *July 17, Reuters* — **Sweltering Midwest has record power demand.** The Midwest Independent Transmission System Operator (ISO) on Monday, July 17, called an emergency alert for conservation in the ISO's western region in the face of heat causing record power demand, a Midwest ISO spokesperson said. The Midwest ISO — which covers part or all of 15 states from Ohio to Montana — set a record for peak demand on Monday at 131,527 megawatts, breaking the previous record of 131,434 MW from August 3, 2005. The emergency alert impacting six utilities in Minnesota, the Dakotas and Montana means conservation measures must be taken to ensure reliable electricity delivery, said Carl Dombek, ISO spokesperson. "We are well prepared for this type of situation. Our operations staff is staying in constant contact with balancing authorities and generation owners to confirm operating needs and capabilities throughout the system," said John Bear, senior vice president and chief operating officer of the Midwest ISO. The six utilities the Midwest ISO specifically called on to conserve were: Northern States Power, Great River Energy, Minnesota Power; Otter Tail Power, Southern Minnesota Municipal Power Agency, and Montana-Dakota Utilities.

Source: [http://news.yahoo.com/s/nm/20060717/us\\_nm/utilities\\_midwest\\_record\\_dc\\_1](http://news.yahoo.com/s/nm/20060717/us_nm/utilities_midwest_record_dc_1)

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

4. *July 18, Burlington Free Press (VT)* — **Ammonia leak in Vermont prompts evacuations.** Mylan Technologies' security guards called 911 Saturday morning, July 15, after smelling ammonia that authorities later identified as coming from Lucille Farm Products, the business next door, in Swanton, VT. The leak of anhydrous ammonia gas forced the evacuation of Mylan Technologies Inc. and 12 homes within four-tenths of a mile from the leak.

Source: <http://www.burlingtonfreepress.com/apps/pbcs.dll/article?AID=/20060716/NEWS02/607160307/1007>

5. *July 18, CBS 4 Boston* — **Rotary re-opens after gas tanker spill.** A busy rotary in Revere, MA, has re-opened, several hours after a gasoline tanker crashed, spilling thousands of gallons of fuel. The truck rolled over Monday evening, July 17, at the intersection of Routes 60 and 107. Crews worked through the night to clean up 3,500 gallons of fuel — some of which spilled into nearby storm drains. Several businesses in the area were evacuated briefly.  
Source: [http://cbs4boston.com/local/local\\_story\\_199065234.html](http://cbs4boston.com/local/local_story_199065234.html)

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

Nothing to report.

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *July 17, Government Computer News* — **No loss of data from VA, USDA breaches.** The Departments of Veterans Affairs (VA) and Agriculture (USDA) have determined that sensitive personal data was not accessed in recent incidents of data threats at both agencies. The FBI has completed its forensic examination of the laptop and hard drive that were stolen from the home of a VA data analyst in May. Based on the results of the forensic tests and other information gathered during the investigation, the FBI indicated that the sensitive files were not accessed or compromised, VA said. The USDA Inspector General's Office (OIG) is conducting an investigation into the computer intrusion. OIG Investigations personnel conducted forensic analysis that indicate that the data file containing personal information about USDA employees was not transferred out of the department's computer system. USDA is conducting a thorough review of all department data systems to minimize the amount of personal information in each system and to confirm that appropriate levels of security are in place.  
Source: [http://www.gcn.com/online/vol1\\_no1/41372-1.html?topic=security](http://www.gcn.com/online/vol1_no1/41372-1.html?topic=security)

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

7. *July 18, Business Review* — **Northwest Airlines plane makes emergency landing at Albany airport.** A Northwest Airlines plane made a successful emergency landing at Albany International Airport on Monday, July 17. Flight 1515 from Albany, NY, to Detroit had just taken off from the airport when the crew identified a problem with one of the DC-9's two engines. The crew decided to return to the airport. While taxiing to the Northwest gate the aircraft experienced some problems with its braking system, according to Albany International Airport spokesperson Doug Myers. The passengers left the aircraft on the runway and were bused to the main terminal.  
Source: <http://biz.yahoo.com/bizj/060717/1316856.html?v=1>

8.

*July 18, Associated Press* — **Governor moves to oust Big Dig chief as tunnel repairs continue.** Massachusetts Governor Mitt Romney served the head of Boston's Big Dig with written allegations of mismanagement and moved forward Tuesday, July 18, in his efforts to oust him, while crews worked to repair a tunnel network where tons of ceiling panels fell, crushing a motorist. Romney has for years been a critic of Matthew Amorello, the chairman and chief executive of the Massachusetts Turnpike Authority, which oversees the massive \$14.6 billion highway project. However, Romney said the fatal accident July 10 bolsters his argument the project has been mismanaged and Amorello should be removed as chief executive. A hearing was scheduled for July 27 on Amorello's dismissal. Romney said he will attend the hearing and listen to Amorello's side before officially deciding his fate. Amorello has the option of contesting the decision in court. Methods for reinforcing heavy concrete ceiling tiles in the Big Dig tunnels were tested successfully Monday and Tuesday, and Romney said he hoped at least one ramp that has been closed since the collapse would be reopened by early next week. Two Big Dig tunnels have since been closed for inspections and repairs since July 10, when 12 tons of ceiling panels fell, killing passenger Milena Del Valle.

Source: [http://www.boston.com/news/local/massachusetts/articles/2006/07/18/romney\\_moves\\_to\\_oust\\_big\\_dig\\_chief\\_as\\_tunnel\\_repairs\\_continue\\_1153252177/](http://www.boston.com/news/local/massachusetts/articles/2006/07/18/romney_moves_to_oust_big_dig_chief_as_tunnel_repairs_continue_1153252177/)

**9. *July 14, Times Dispatch (VA)* — Demand seen for express buses to Fredericksburg.**

Richmond, VA, residents weary of driving Interstate 95 could soon have another way to get to Washington, DC. GRTC Transit System is exploring possible express bus service into Fredericksburg, VA, where commuters could hop on the Virginia Railway Express (VRE) before continuing to Northern Virginia and Washington. John Lewis Jr., chief executive officer for GRTC, said the company expects to request bids from private bus companies in September. The bids should determine whether the service could be operated with passengers picking up the entire cost, he said. If all goes well, the buses could start rolling by late October or November with two morning and two afternoon trips Monday through Friday, Lewis said. VRE estimates it has about 100 regular riders from the Richmond area who board at the Fredericksburg station, the southern end of the commuter rail system. Lewis believes express buses could attract as many as 130 riders by also drawing some from vanpools, plus those commuters traveling from Fredericksburg to Richmond. VRE recognizes the market for riders from Richmond and believes it will increase only if service is extended farther south into Spotsylvania and Caroline counties, VRE spokesperson Mark Roeber said.

Source: [http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD\\_BasicArticle&c=MGArticle&cid=1149189143452&path=%21news&s=1045855934842](http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1149189143452&path=%21news&s=1045855934842)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

- 10. *July 18, USA TODAY* — Lower 9th Ward finally gets mail delivery.** The rest of America takes the mail for granted. But in the Lower 9th Ward of New Orleans, where Katrina's flooding reached rooftops and pushed houses off foundations, the first round of mail delivery — Monday, July 17 — carried some hope for normalcy in a place where normal is hard to come by. The Lower 9th Ward, once home to about 20,000, is one of the last New Orleans neighborhoods where basic services remain scarce. It's the only neighborhood in the city where

electricity and gas services have not been fully restored. Government-issue travel trailers began showing up just last month. One section of the neighborhood, nearest the levee breach, remains essentially closed, with no lights or even drinkable water. It is dotted with empty lots where houses once stood. That makes mail delivery a big deal for the residents — fewer than 1,000 — who have returned. After a complete disruption in mail service following Katrina, the post office began over-the-counter pickup service in October. Delivery, albeit slow and erratic, began in unflooded neighborhoods later in the fall. No one was receiving magazines until May. Source: <http://www.usatoday.com/news/nation/2006-07-17-mail-ninth-wa rd x.htm>

[[Return to top](#)]

## **Agriculture Sector**

11. *July 17, Animal and Plant Health Inspection Service* — **Plum pox virus confirmed in New York.** The U.S. Department of Agriculture's National Plant Germplasm and Biotechnology Laboratory in Beltsville, MD, Monday, July 17, confirmed the presence of the plum pox virus (PPV) on plum tree leaf samples collected by New York State Department of Agriculture and Markets officials. As part of a seven-year survey for the virus, state and federal agriculture officials collected 22 leaf samples from a 108-tree orchard located in Niagara County, NY — within five miles of plum pox eradication zones in Canada. The samples were sent to Cornell University's diagnostic laboratory for testing, where researchers obtained positive results. The virus was first detected in Canada back in 2000. The plum pox strain identified in New York is identical to the D strain of the virus found in both Canada and Pennsylvania. The D strain of the virus is less virulent than other strains, making it easier to contain. Survey specialists are currently surveying a five-mile radius surrounding the initial detection to determine the extent of infestation. The U.S. Department of Agriculture will establish a cooperative eradication program with the state of New York.

Plum pox virus information: <http://plantclinic.cornell.edu/FactSheets/plumpoxvirus/plumpox.htm>

Source: <http://www.aphis.usda.gov/newsroom/content/2006/07/plumpox.s.html>

12. *July 17, Stop Soybean Rust News* — **More soybean rust found on kudzu in Brooks County, Georgia.** Georgia officials said soybean rust was found Monday, July 17, on a sample collected from kudzu in Brooks County, southeast of Quitman, GA. Rust was first found on kudzu in the county on June 29, 2006. Officials said the find in south-central Georgia on the Florida border was collected from a shaded area under pine trees. The sample was "brought in, examined and confirmed with a dissection microscope. Six leaves were examined, and all six leaves were infected with sporulating soybean rust pustules. Soybean rust had already been confirmed in the same county on kudzu at a different location.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=883>

[[Return to top](#)]

## **Food Sector**

13.

*July 17, Food Safety and Inspection Service* — **Beef recalled.** George G. Ruppersberger & Sons, Inc., a Baltimore, MD, firm, is voluntarily recalling approximately 315 pounds of ground beef that may be contaminated with E. coli O157:H7. The problem was discovered through routine Food Safety and Inspection Service (FSIS) microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. The ground beef was produced on July 13 and was distributed to restaurants and institutions in Baltimore, MD. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration. Source: [http://www.fsis.usda.gov/News\\_&\\_Events/Recall\\_021\\_2006\\_Relea se/index.asp](http://www.fsis.usda.gov/News_&_Events/Recall_021_2006_Relea se/index.asp)

[[Return to top](#)]

## **Water Sector**

Nothing to report.

[[Return to top](#)]

## **Public Health Sector**

### **14. *July 17, Vanderbilt University* — Vanderbilt participating in West Nile vaccine trial.**

Vanderbilt University Medical Center researchers, in collaboration with investigators at Johns Hopkins University, are beginning a Phase I trial to test a new vaccine against the West Nile virus. “When West Nile virus first appeared in the U.S. five or six years ago, it spread remarkably quickly across the country,” said Peter Wright, who is heading up Vanderbilt’s efforts in the trial. “There’s no part of the country that has not experienced human and bird cases of West Nile.” There are currently no specific treatments or vaccines to combat West Nile infection, so those infected are consigned to letting the illness run its natural course. While it is not clear who would most benefit from a West Nile vaccine, Wright suggests that it could be beneficial to certain high-risk populations, such as the elderly, people who work outside and have frequent exposure to mosquitoes, or those in specific geographic regions where West Nile cases are detected. Finding an effective vaccine against West Nile could also open doors to developing vaccines for other insect-borne illnesses like Dengue fever, which are a priority for vaccine development because of their considerable global impact.

West Nile virus information: <http://www.cdc.gov/ncidod/dvbid/westnile/index.htm>

Source: <http://www.vanderbilt.edu/news/releases/2006/7/17/vanderbilt-participating-in-west-nile-vaccine-trial>

### **15. *July 17, Associated Press* — Architects endorse private hospital rooms.** Private rooms would be standard in new U.S. hospitals under recommendations from an architects' group that says building design can help curb infectious diseases and medical errors. Recommendations on hospital design from the American Institute of Architects are used as the basis for regulations in 42 states, and private rooms are increasingly favored by hospitals nationwide to address safety, noise and privacy issues, said Dale Woodin of the American Hospital Association. Woodin is on a panel of the architects institute that created the 2006 guidelines. The panel includes doctors, hospital administrators, infection control experts, engineers and architects who voted unanimously to adopt the recommendations.

Source: <http://news.moneycentral.msn.com/provider/providerarticle.as>



16. *July 17, Associated Press* — **Namibia launches polio vaccine campaign.** During an official check to certify that Namibia remained polio-free a decade after it declared it had conquered the disease, officials made a surprising find: A 39-year-old man stricken with the virus. Since that first case in May, Namibia has detected 185 suspected cases — including 21 deaths — and 17 confirmed cases. Unusually for a disease that mainly strikes children, most of the cases have been adults. The Namibian government on Tuesday, July 18, will launch a three-day nationwide immunization drive aiming to vaccinate the entire population. Health officials say about 75 percent of the suspected cases are over 15 — a reflection of the fact that only children have been vaccinated under a routine immunization campaign Namibia launched in 1990. Global Polio Eradication Initiative: <http://www.polioeradication.org/>  
Source: <http://www.cbsnews.com/stories/2006/07/17/ap/health/mainD8IT RHVO0.shtml>
17. *July 14, Associated Press* — **New Mexico girl contracts bubonic plague.** A girl from Bernalillo County has contracted bubonic plague — the fourth case of plague in New Mexico this year. She is being treated at the University of New Mexico Hospital. The Albuquerque Environmental Health Department says it will conduct an investigation at the girl's home to assess any possible risk for other people to contract the illness. Bubonic plague information: <http://www.cdc.gov/ncidod/dvbid/plague/index.htm>  
Source: <http://www.kobtv.com/index.cfm?viewer=storyviewer&id=26774&cat=NMTOPSTORIES>

[\[Return to top\]](#)

## **Government Sector**

18. *July 18, Government Accountability Office* — **GAO-06-885T: Global War on Terrorism: Observations on Funding, Costs, and Future Commitments (Testimony).** After the terrorist attacks of September 11, 2001, the President announced a Global War on Terrorism (GWOT), requiring the collective instruments of the entire federal government to counter the threat of terrorism. Ongoing military and diplomatic operations overseas, especially in Iraq and Afghanistan, constitute a key part of GWOT. These operations involve a wide variety of activities such as combating insurgents, civil affairs, capacity building, infrastructure reconstruction, and training military forces of other nations. The U.S. has reported substantial costs to date for GWOT related activities and can expect to incur significant costs for an unspecified time in the future, requiring decision makers to consider difficult trade-offs as the nation faces increasing long-range fiscal challenges. The Government Accountability Office (GAO) has issued several reports on current and future financial commitments required to support GWOT military operations, as well as diplomatic efforts to stabilize and rebuild Iraq. This testimony discusses (1) the funding Congress has appropriated to the Department of Defense (DOD) and other U.S. government agencies for GWOT-related military operations and reconstruction activities since 2001; (2) costs reported for these operations and activities and the reliability of DOD's reported costs, and (3) issues with estimating future U.S. financial commitments associated with continued involvement in GWOT. Highlights: <http://www.gao.gov/highlights/d06885thigh.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-885T>

19. *May 03, Council on Foreign Relations* — **Report: Government failing to mobilize private sector in homeland security efforts.** A special report by the Council on Foreign Relations begins by laying out the policy dilemma in detail, offers a recent history of the security role of the private sector, highlights specific problems that have kept the public–private relationship from maturing, and offers a series of principles for a more productive relationship. It concludes with a series of specific recommendations — some will be the work of Congress, others the purview of the administration, still others the responsibility of the private sector — to secure the homeland better. Among its conclusions, it states that to make America more secure, the federal government urgently needs to provide better leadership on homeland security issues and become an active partner with the private sector on target protection, preparedness, response, and recovery.

Report: <http://www.cfr.org/publication/10457/>

Source: [http://www.cfr.org/publication/10570/us\\_government\\_failing\\_to\\_mobilize\\_private\\_sector\\_in\\_homeland\\_security\\_efforts\\_warns\\_council\\_special\\_report.html?breadcrumb=default](http://www.cfr.org/publication/10570/us_government_failing_to_mobilize_private_sector_in_homeland_security_efforts_warns_council_special_report.html?breadcrumb=default)

[[Return to top](#)]

## **Emergency Services Sector**

20. *July 18, Associated Press* — **DHS asks Louisiana to detail storm–evacuation needs.** The Bush administration said Monday, July 17, that it needs specific lists of Louisiana's shelters, immobile hospital patients and transportation pickup points before it can promise reliable evacuation help during a major hurricane. In a letter to Governor Kathleen Babineaux Blanco, Department of Homeland Security (DHS) Secretary Michael Chertoff made clear what responsibilities the federal government will shoulder the next time a huge storm strikes. Chertoff gave the state a deadline of Wednesday, July 26, to provide the lists. The needed information, according to Chertoff's letter, includes: a) places in southeastern Louisiana where evacuees can be picked up by federally provided transportation and taken to shelters, rail stations or airports; b) all available and adequate shelters in the state; c) an accurate facility–by–facility count of medical patients who will need federal help in evacuating or finding shelter.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/17/AR2006071701370.html>

21. *July 18, Billings Gazette (MT)* — **Montana schools begin work on disaster plans.** The Montana University System is working on the first of several projects to mitigate the effects that a natural or technological disaster would have on Montana campuses. Pre–Disaster Mitigation Plans are being developed to identify the hazards for each campus. The information will be used to identify and prioritize mitigation actions. Campuses involved in this first phase of such planning are Montana State University (MSU)–Billings, MSU, Montana Tech in Butte, University of Montana (UM)–Western in Dillon, MSU–Great Falls College of Technology, MSU–Northern in Havre, UM Helena College of Technology's airport campus and the main UM campus in Missoula. The plans will conform with the Federal Disaster Mitigation Act of 2000.

Source: <http://www.billingsgazette.net/articles/2006/07/18/news/stat e/48–schools.txt>



**22. July 18, *Federal Emergency Management Agency* — Federal Emergency Management Agency National Situation Update.** Tropical Activity: Eastern Pacific: Tropical Storm 05E (Daniel) is south of the Baja Peninsula, moving west out to sea and forecast to become a hurricane Tuesday, July 18. Based on the current warning this system does not pose a threat to the U.S. or its territories.

Tropical Depression 04E (Carlotta) has dissipated over water.

Western Pacific: Tropical Depression 06W has formed in the Pacific southeast of Guam.

Tropical Depression 06W is expected to continue a northwest motion passing about 150 miles southwest of Guam.

Earthquake Activity: Internationally, significant earthquakes and aftershocks continue near Java, Indonesia, following Monday's 7.7 earthquake.

To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>

Source: <http://www.fema.gov/emergency/reports/2006/nat071806.shtm>

**23. July 17, *Providence Journal (RI)* — Rhode Island slow in raising public awareness.** Rhode Island completed a hurricane response plan just in time for this year's hurricane season, which began on June 1. But it failed to meet its next most important goal — informing the public. Governor Carcieri said in May that he wanted it done — fast. He wanted preparedness tips and maps of the evacuation routes mailed to every house in a coastal flood zone. Robert Warren, director of the state's Emergency Management Agency (EMA), said he planned to launch the publicity campaign by mid-June. Neither goal has been met. Right now the state is trying to heighten public awareness using a few thousand copies of an old brochure that depicts a hurricane on the cover with a happy face. An early version included an old Internet address for the state's EMA Website that no longer exists. Armand Randolph, the EMA's public information officer, said last week he is doing the best he can in the time available. Randolph has been working on a public outreach campaign since the evacuation maps were published online in February. One problem, he said, is that he can't figure out how to get addresses just for homes in the flood zones.

Source: [http://www.projo.com/news/content/projo\\_20060717\\_warn17.17f0.082.html](http://www.projo.com/news/content/projo_20060717_warn17.17f0.082.html)

**24. July 17, *Palm Beach Post (FL)* — Red Cross chapters fret about revamp.** Dogged by criticism about inefficiencies and lack of communication and cooperation with other agencies, the American Red Cross is working on an initiative that leaders hope will streamline operations and bring increased services into under-served communities. But how it will all go down is the big unknown, and that has some local chapter leaders wondering about their futures. Dubbed the "community initiative," the plan was hatched in 2004, but recent problems stemming from Hurricane Katrina have made the planned overhaul of operations for the nation's 800 chapters even more relevant, Red Cross officials said. The idea being floated at the national level is to make the larger chapters responsible for the administrative functions of the smaller chapters, leaving the smaller chapters to focus on providing services such as first-aid training and emergency and disaster assistance. Those selected as regional chapters will then report to the Red Cross' eight regional offices around the country.

Source: [http://www.palmbeachpost.com/storm/content/local\\_news/epaper/2006/07/17/s1b\\_redcross\\_0717.html](http://www.palmbeachpost.com/storm/content/local_news/epaper/2006/07/17/s1b_redcross_0717.html)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

25. *July 18, Washington Post* — **To agency insiders, cyber thefts and slow response are no surprise.** To government officials responsible for information security and to outside experts, intrusions into government Websites is no surprise. Over the past several years, some agencies have received failing grades on a congressional report card for their information–security practices. The overall grade for federal agencies in 2005 was D–plus. Officials and experts say that the frequency of the recent security incidents is not unusual, and that much more work needs to be done in the federal government to implement effective cybersecurity policies. In fiscal 2005, major federal agencies reported about 3,600 incidents that were serious enough to warrant alerting the government's cybersecurity center at the Department of Homeland Security, including 304 instances of unauthorized access and 1,806 cases of malicious computer code, according to a yearly Office of Management and Budget report. But that does not present a full picture. Despite requirements to do so, agencies are "not consistently reporting incidents of emerging cybersecurity threats," government auditors said last year.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/17/AR2006071701170.html>
26. *July 17, Security Focus* — **Mozilla Suite, Firefox, SeaMonkey, and Thunderbird multiple remote vulnerabilities.** The Mozilla Foundation has released nine security advisories specifying security vulnerabilities in Mozilla Suite, Firefox, SeaMonkey, and Thunderbird. Analysis: These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application. Crash affected applications, gain elevated privileges in JavaScript code, potentially allowing remote machine code execution. Gain access to potentially sensitive information, bypass security checks, and spoof window contents.  
For a complete list of vulnerable products: <http://www.securityfocus.com/bid/17516/info>  
Solution: New versions of the Mozilla Suite, Firefox, SeaMonkey, and Thunderbird are available to address these issues. Most Mozilla applications have self–updating features that may be used to download and install fixes. For information on obtaining and applying fixes: <http://www.securityfocus.com/bid/17516/references>  
Source: <http://www.securityfocus.com/bid/17516/discuss>
27. *July 17, Security Focus* — **Microsoft ISA server file extension filter bypass vulnerability.** Microsoft Internet Security and Acceleration (ISA) Server is prone to a vulnerability that may let users bypass rules for filtering file extensions. Analysis: Attackers could exploit this vulnerability to bypass administrative policy and to access restricted content on the Internet. Vulnerable: Microsoft ISA Server 2004.  
Solution: Currently, Security Focus is not aware of any vendor–supplied patches for this issue.  
Source: <http://www.securityfocus.com/bid/18994/references>
28. *July 17, Security Focus* — **Microsoft Works Spreadsheet multiple remote vulnerabilities.** The spreadsheet component of Microsoft Works is prone to multiple remote vulnerabilities. Analysis: These issues occur because the application fails to handle specifically crafted spreadsheet documents when importing them into Microsoft Works. These vulnerabilities allow remote attackers to execute arbitrary machine code in the context of affected application. Attackers may also crash vulnerable applications, denying service to legitimate users. Microsoft

Works version 8.0 is vulnerable to these issues; other versions may also be affected.

Vulnerable: Microsoft Works 8.0.

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/18989/references>

**29. *July 17, Security Focus* — Microsoft PowerPoint multiple unspecified vulnerabilities.**

Microsoft PowerPoint is prone to multiple remote vulnerabilities. Three proof-of-concept exploit files designed to trigger vulnerabilities in PowerPoint have been released. It is currently unknown if these three exploit files pertain to newly discovered, unpublished vulnerabilities or if they exploit previously disclosed issues. These issues may allow remote attackers to cause crashes or to execute arbitrary machine code in the context of the affected application, but this has not been confirmed. This BID will be updated and potentially split into individual records as further analysis is completed. Microsoft PowerPoint 2003 is vulnerable to these issues; other versions may also be affected. For more information on vulnerabilities:

<http://www.securityfocus.com/bid/18993/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for these issues.

Source: <http://www.securityfocus.com/bid/18993/references>

**30. *July 17, ihotdesk* — Trojan horse masquerades as message of love.** An e-mail attachment containing a number of loosely philosophical ponderings on the art of love is threatening businesses and home computer users across the world. This latest online attack contains a malicious Microsoft PowerPoint file that is able to exploit an unpatched vulnerability in the software. The file contains exploit code that drops the Troj/Edepol-C keylogging Trojan, which in turn allows the hacker to spy on computer users. This particularly irritating Trojan horse also tries to disable anti-virus products running on the infected computer, which only aggravates the threat.

Source: <http://www.ihotdesk.com/article.asp?ID=17342122>

**31. *July 17, National Journal's Technology Daily* — OMB publishes online catalog of IT guidelines.** Part of the challenge of implementing change is following the guidelines — and knowing exactly what the changes are. To that end, the White House Office of Management and Budget (OMB) on Monday, July 17, announced the release of an online catalog to make guidelines on information technology practices easier to access. OMB is sending a memorandum to the chief information officers and chief architects of the different federal agencies to explain the launch of the federal transition framework, which consolidates guidance to agencies on policies and best practices on tech solutions.

OMB's online catalog: <http://www.whitehouse.gov/omb/egov/a-2-EAFTF.html>

Source: [http://www.govexec.com/story\\_page.cfm?articleid=34571&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=34571&dcn=to%20daysnews)

## **Internet Alert Dashboard**

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

**VU#936945:** Microsoft PowerPoint contains an unspecified remote code execution vulnerability. <http://www.kb.cert.org/vuls/id/936945>

US-CERT strongly recommends the following until an update, patch, or more information becomes available:

Do not open attachments from unsolicited email messages.

Install anti virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments. <http://www.us-cert.gov/cas/tips/ST04-010.html>

US-CERT will continue to update current activity as more information becomes available.

#### **PHISHING SCAMS**

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.  
[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

#### **Current Port Attacks**

<b>Top 10 Target Ports</b>	1026 (win-rpc), 26777 (---), 38566 (---), 445 (microsoft-ds), 32790 (---), 80 (www), 113 (auth), 135 (epmap), 25 (smtp), 4672 (eMule) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[[Return to top](#)]

## **General Sector**

**32. *July 18, Associated Press* — Sweltering heat to persist until weekend.** The heat wave that has gripped most of the nation showed few signs of abating Tuesday, July 18, and may persist for some regions until the weekend. Temperatures predicted to soar past 100 degrees in parts of the Plains, Great Basin, Desert Southwest and California Valley. Scores of communities reported temperatures of more than 100 degrees: Redding, CA, about 160 miles north of Sacramento, reached 110 degrees; Grand Junction in western Colorado hit 101; Russell, KS, hit 108. One of LaGuardia International Airport's four terminals and part of a second lost power in New York when high demand caused by the heat triggered equipment problems. In Illinois, state officials made more than 130 office buildings available as cooling centers. Detroit cranked up the air conditioning in 11 of its libraries and invited the public to take refuge from the heat. In Kentucky, Louisville officials offered free fans or air conditioners to those in immediate need. Source: [http://www.usatoday.com/weather/news/2006-07-17-heat-wave\\_x.htm](http://www.usatoday.com/weather/news/2006-07-17-heat-wave_x.htm)

[[Return to top](#)]

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.